High Performance Elliptic Curve GF(2/Sup K/) Cryptoprocessor Architecture For Multimedia

Gutub, A.A.-A. Ibrahim, M.K.; Dept. of Comput. Eng., King Fahd Univ. of Pet. & Miner., Dhahran, Saudi Arabia;

Multimedia and Expo, 2003. ICME '03. Proceedings. 2003 International conference;Publication Date: 6-9 July 2003;Vol: 3,On page(s): III- 81-4 vol.3;ISBN: 0-7803-7965-9

King Fahd University of Petroleum & Minerals

http://www.kfupm.edu.sa

Summary

A high performance GF(2/sup k/) elliptic curve crypto processor architecture suitable for multimedia security is proposed. To meet the high data rates of multimedia, the new architecture exploits parallelism within elliptic curve point operations after using projective coordinates. In this paper, the decision on which projective coordinate to use is based on its efficiency with regard to its parallel implementation. Two different projective coordinates are compared here. This parallelism is exploited in the new architecture by using three separate bit-level pipelined digit serial-parallel multipliers that can operate in parallel. It is worth pointing that such multipliers are ideally suited for the repetitive multiplications inherent in elliptic curve cryptography. it is believed that such high performance architectures are needed for high end servers that need to support the security of many multimedia streams at the same time.